الجدار الناري Fire Wall بويندوز XP بروفيشينال (دورة دراسية خاصة)

أعداد المبرمج :مشتاق طالب رشيد العامري

Mushtaq_talib58@yahoo.com



٢٠٠٩

شركة الأميرال للبرمجة المتطورة

الجدار الناري Fire Wall بويندوز XP بروفيشنال (دورة دراسية خاصة)

يتوفر بإصدارة ويندوز XP بروفيشينال (الخاصة بالأعمال) جدارا ناريا صلدا من اهم مهامة الأساسية

١- التخفي Stealth
٢- العمل بقوة في صمت دون مقاطعة المستخدم
٣- مساندة الشبكات المحلية
٤- الإستغناء كليا وبمصداقية عن تحميل اي تطبيقات خارجية (جدران نارية) لصد عمليات الإختراق
٥- سهولة التحميل والتهيئة والعمل في الخلفية دون ادنى تدني لسرعة الجهاز
٦- التحديث التلقائي ضمن تحديثات ويندوز XP الدورية
٧- الإختبار الفعلي للنظام عبر مركز جيبسون للأبحاث com.grc.www

سأبداء بشرح مفاهيم الجدار الناري الذاتي بالويندوز XP بروفيشينال ووميزاته والفروقات الواضحة والخفيه بينه وبين بقية تطبيقات الجدران النارية المتداوله

الحلقة الدراسية الأولى

تعريف الجدار الناري :

الجدار الناري او جدار الحماية او Firewall سمه كما تشاء هو تركيبة من الأجهزة والبرامج التي توفر نظام آمن ، تُستخدم عادةً لمنع الوصول غير المصرح به من الخارج إلى شبكة اتصال داخلية أو إنترانت.
يمنع جدار الحماية الاتصال المباشر بين شبكة الاتصال وأجهزة الكمبيوتر الخارجية بواسطة توجيه الاتصال عبر ملقم وكيل خارج شبكة الاتصال . يقرر الملقم الوكيل فيما إذا كان مرور ملف ما عبر شبكة الاتصال آمناً. يدعى جدار الحماية أيضاً عبارة الحد الآمن.

إن الجدار الناري Firewall هو نظام الأمان الذي يعمل كحد وقائي بين شبكة الاتصال والعالم الخارجي . إن جدار حماية اتصال إنترنت ICF -Connection Firewall Internet هو برنامج لتعيين قيود على نوعية المعلومات المتبادلة بين الشبكة المنزلية أو المكتبية الصغيرة وإنترنت.

يمكن لـ ICF أن يحمي الكمبيوتر المفرد المتصل بإنترنت . إذا كان لديك كمبيوتر مفرد متصل بإنترنت بواسطة مودم الكيبل ، أو مودم DSL ، أو مودم الطلب الهاتفي ، يقوم ICF بحماية اتصالك بالإنترنت .

كيفية عمل جدار حماية اتصال إنترنت (ICF) :

يراقب جدار الحماية كافة أوجه الاتصالات التي تعبر مساره ويختبر عنوان الوجهة والمصدر لكل رسالة يعالجها. لمنع حركة المرور غير المطلوبة من الطرف العام للاتصال من دخول الطرف الخاص، يحتفظ ICF بجدول لكافة الاتصالات التي تم إجراؤها من كمبيوتر ICF. في حالة الكمبيوتر المفرد، يتتبع ICF حركة المرور الخاصة بالكمبيوتر. عند استخدامه مع ICS، يتتبع ICF كامل حركة المرور الخاصة بكمبيوتر ICS/ICF والخاصة بأجهزة كمبيوتر شبكة الاتصال الخاصة. تتم مقارنة حركة المرور الواردة من إنترنت مع الإدخالات في الجدول. ويتم السماح لحركة مرور إنترنت الواردة بالوصول إلى أجهزة الكمبيوتر الموجودة على شبكة الاتصال عند وجود إدخال مطابق في الجدول الذي يظهر بدء تبادل الاتصال من ضمن الكمبيوتر أو شبكة الاتصال الخاصة.

يتم إسقاط الاتصالات الناتجة من مصدر خارج كمبيوتر ICF، كإنترنت مثلاً، من قبل جدار الحماية إلا إذا تم إنشاء إدخال في التبويب الخدمات للسماح بالمرور. وعوضاً عن إرسال إعلامات حول النشاط، يقوم ICF بصمت بتجاهل الاتصالات غير المطلوبة، مع إيقاف المحاولات الشائعة للقرصنة مثل مسح المنفذ. إذ أنه يمكن إرسال هذا النوع من الإعلامات بشكل متكرر مما يؤدي إلى تعطيلك عن العمل. عوضاً عن ذلك، يمكن أن يقوم ICF بإنشاء سجل أمان لعرض النشاط المتتبع من قبل جدار الحماية.

يمكن تكوين الخدمات للسماح بإعادة توجيه حركة المرور غير المطلوبة من إنترنت من قبل كمبيوتر ICF إلى شبكة الاتصال الخاصة. على سبيل المثال، إذا كنت تستضيف خدمة ملقم ويب HTTP، وقمت بتمكين الخدمة HTTP على كمبيوتر ICF، فسيتم إعادة توجيه حركة مرور HTTP غير المطلوبة من قبل كمبيوتر ICF إلى ملقم ويب HTTP. تكون مجموعة معلومات العمل والمعروفة بتعريف الخدمة مطلوبة من قبل ICF للسماح بإعادة توجيه حركة مرور إنترنت غير المطلوبة إلى ملقم ويب على شبكة الاتصال الخاصة. لمزيد من المعلومات حول الخدمات، راجع إضافة تعريف الخدمة، و نظرة عامة حول تعريفات الخدمات.

ماذا نستنتج من السطور اعلاه ؟ :

الغازاً ؟ !! ... لا .. ليس بألغاز بقدر ماهي ميكانيكية برمجية على كل متصل بالانترنت التعرف عل اسسها ومبادئها ، ببساطة توفر الجدران النارية المتداوله كالزون الارم والكلين والبلاك ايس ديفندر واللوك داون وغيرها حماية مفردة اي تكون في مجملها جدارا ناريا خاصا بالمستخدم العادي الذي يستخدم كمبيوتر شخصي وحيد ، ولكنها لاتحمي الشبكات سواء المنزلية او الخاصة بالأعمال ، بصيغة اخرى لو أن زيد من الناس ركب شبكة منزلية في بيته مكونه من خمسة اجهزة فسيتعين عليه إستخدام نظاما خاصا لحماية الشبكة ثم تحميل جدار ناريا مفردا لحماية كل جهاز على حده وفوق ذلك عليه اعادة تهيئة كل جدارناري على حدة حتى يتم نجاح اتصال الأجهزة ببعضها عبر الشبكة الداخليه ، لأن الجدران النارية توقف تواصل الأجهزة مالم يتم تهيئتها لذلك.

تختلف طريقة الجدار الناري الخاص بالويندوز XP في طريقة تعامله مع الشبكات ، حيث يقدم حماية مزدوجة القوة للأجهزة الشخصية المرتبطة بالشبكة وللشبكة ذاتها كما هو مشروح اعلاه ، دون التعرض لإتصال الأجهزة الفردية بعضها ببعض عبر الشبكة الداخلية من جانب ، وإتصال الشبكة الداخلية بالأنترنت من جانب أخر.

التخفي Stealth :

لمعرفة مصطلح التخفي في الإنترنت علينا أن نتعرف على ميكانيكية المطاردة والصيد Hunting & Chasing ، حيث يقوم المخترق بأرسال رسالة إستعلامية مرجعية PING عبر تطبيقات الإختراق ليتسنى له تحديد ارقام الأيبي IPs بالأجهزة ذات المنافذ المفتوحة open ports وهذة دلالة واضحة على ان اصحابها لايحملون بها جدراناً نارية او انهم محملين لجدران نارية إلا ان ملفات تجسسة من نوع احصنة طروادة Trojans قد تم زراعتها بأجهزتهم بطريقة او أخرى وقد تمكنت من فتح بعض المنافذ للغزاة . في هذة العجالة نستنتج امرين ، الأول ان الجدران النارية تقوم بوضع كتل صلدة في وجة رسائل الـ PING ، كذلك تغلق المنافذ التي تبحث عن ثغراتها تلكم الرسائل المرجعية خلال عملية المطاردة والصيد Chasing & Hunting.

مايميز جدار الحماية بويندوز XP هو عامل التخفي Stealth وهذة الكلمة الإنجليزية اشتهرت بأسم الطائرة الشبح من نوع F18 التي انتجتها امريكا والتي لايستطيع الرادار ان يتصيدها . من هنا تقترن كلمة Stealth بالجدرا الناري المزود بالويندوز XP بروفيشينال وقد وضعته مايكروسوفت في نسخة الأعمال من الويندوز إكس بي ولم تزود به نسخة الهوم إديتشن لأن الأولى مرتبطة بالشبكات ، والشبكات بحاجة الي حماية من كل وسائل وطرق الإختراق المتعارف عليها ، وعليه فإن الجدار الناري هذا يشكل عامل تخفي عجيب حيث لا تكتشف الرسائل المرجعية PINGs اجهزة الكمبيوتر التي تستخدمة وكأنها - اي الكمبيوترات - غير متصلة اساسا بالأنترنت.

الإختبار التجريبي الفعلي :

إن عملية الحماية المزدوجة التي يقدمها الجدار الناري في الويندوز XP بروفيشينال بما فيها من عامل التخفي Stealth يمكن التحقق من ادائها ونجاحها عبر الإختبار الذي يوفره مركز جيبسون للأبحاث Gibson's Research Center عبر الرابط التالي :

exe.leaktest/files/com.grc//:http

انزل برنامج LeakTest واجرى الفحص خلال تنشيط الجدار الناري .

ستحصل على نتيجة كالتالي :

Unable To Connect

.COM Web Server.LeakTest was unable to connect to the GRC

لماذا ؟؟

لأن الجدار الناري الخاص بالويندوز XP جعل جهازك مخفياً كالشبح Stealth كأنما هو غير مرتبط بالأنترنت ، ولذا لم يتمكن سيرفر مركز ابحاث جيبسون من تحديده لتنفيذ الأختبار.

يمكنك شخصيا إجراء إختبار فعلي مماثل للتحقق من فعالية تخفي النظام ، بعد تنشيط الجدار الناري - سنتطرق لهذة العملية بالتفصيل في الحلقة الدراسية القادمة إن شاء الله - حمل جدارا ناريا أخرا بجانب جدار ويندوز XP الناري وراقب ايقونيته ... ستجد انها لاتغمز البته ، وإن حدث وهو نادرا فالسبب اما يعود الي سيرفر مزود الخدمة او الي نشاط الداتا المرسلة من جهازك outbound connections وليست المرسله اليه ، هناك فرق . حسنا ، اوقف خاصية الجدار الناري بالويندوز XP وراقب كم مرة تغمر ايقونية الجدار الناري الخارجي؟؟ ... كثيرا .. اليس كذلك ؟! ... الأن فقط ... أنت الحكم.

الحلقة الدراسية الثانية

تنشيط خيارات سجل الأمان :

تعودنا جميعا عند تحميل الجدران النارية التقليدية مراقبة ايقونية الجدار الناري لملاحظة محاولات الأختراق المضنية ومن ثم متابعة المخترق لتحديد موقعة عبر رقم الأي بي ومعرفة التطبيق الذي يستخدمه للأختراق . ولأننا تعودنا على ذلك فأننا لن نشعر بالأطمئنان في بداية إستخدامنا لجدار مايكروسوفت ويندوز XP الناري ، فلا وجود لإيقونيات تغمز لأرشادنا لتتبع محاولات الإختراق ، ولا وجود لسجل امان معين نضغط على ايقونية التطبيق لنفتحة ونشاهد تلك المحاولات. لماذا ؟ ، بكل بساطة لأن الجدار الناري هذا يختلف في طريقة عمله عن بقية الجدران النارية التقليدية ، فليس من مهامة الرئيسية تحديد محاولات الإختراق وكشف التطبيقات التي يستخدمها المخترقون ، بل هو أسمى من ان يتحسس ميكانيكية الإختراق لأن ليس هناك ميكانيكة للأختراق من الأساس حيث انه يخفي جهاز المستخدم Stealth وكأنما هو ليس بمتصل بالانترنت البته ، وعليه فإن محاولات المخترقين تطارد شبحا في هذه الحالة. على كل حال ، يحتفظ الجدار الناري بسجل خاص لمحاولات الإختراق إن وجدت ، ولكنه لايقاطع المستخدم بالتغميز او إصدار لصوت تنبيهي عند صد كل محاولة للأختراق كما تفعل الجدران النارية التقليدية ، وإنما يعمل في الخلفية دون اية مقاطعة للمستخدم ومتى ما رغب المستخدم في التعرف على سجل محاولات الأختراق للشبح ، فعلية في هذة الحالة فقط الإطلاع على السجل الأمني يدويا وستفاجأه الحقيقة لأنه سيجد السجل فارغا حيث ليس هناك من الأساس صد لمحاولات إختراق لكمبيوتر شبحي.

يسمح سجل أمان جدار حماية اتصال إنترنت (ICF) للمستخدمين المتقدمين باختيار المعلومات الواجب تسجيلها. باستخدام تسجيل أمان ICF يمكنك:

تسجيل الحزم المسلّمة. سيسجّل هذا كافة الحزم المسقطة التي تنشأ من شبكة الاتصال المنزلية أو المكتبية الصغيرة أو من إنترنت. تسجيل الاتصالات الناجحة. سيسجّل هذا كافة الاتصالات الناجحة التي تنشأ من شبكة الاتصال المنزلية أو المكتبية الصغيرة أو من إنترنت.

عند تحديد خانة الاختيار تسجيل الحزم المسلّمة، يتم جمع معلومات حول كل محاولة حركة المرور للانتقال عبر جدار الحماية يتم الكشف عنها ورفضها من قبل ICF. على سبيل المثال، عند عدم تعيين إعدادات بروتوكول رسائل تحكم إنترنت (ICMP) للسماح بطلبات الارتداد الواردة، مثل تلك المرسلة من قبل أوامر Ping، و Tracert، وتم تلقي طلب الارتداد من خارج شبكة الاتصال، يتم إسقاط طلب الارتداد، ويتم إنشاء إدخال في السجل. عند تحديد خانة الاختيار تسجيل الاتصالات الناجحة، يتم جمع معلومات حول كل اتصال ناجح للتنقل عبر جدار الحماية. على سبيل المثال، عند اتصال شخص ما بنجاح بموقع ويب باستخدام Internet Explorer، يتم إنشاء إدخال في السجل. يتم إنشاء سجل الأمان باستخدام تنسيق W3C Extended Log File Format، يتم استخدام تنسيق مشابه للتنسيق المستخدم في أدوات تحليل السجل الشائعة. للحصول على معلومات حول كيفية عرض سجل أمان ICF، راجع عرض سجل الأمان. لحفظ سجل جدار الحماية باستخدام اسم وموقع من اختيارك، راجع تغيير اسم الملف والمسار لسجل الأمان.

لدى سجل أمان جدار حماية اتصال إنترنت مقطعين:

توفر معلومات العنوان معلومات حول إصدار سجل الأمان والحقول المتوفرة لإدخال البيانات. تعرض معلومات العنوان كقائمة ثابتة. إن نص سجل الأمان هو البيانات المترجمة والتي تم إدخالها كنتيجة لمحاولة حركة المرور عبور جدار الحماية. يتم إدخال الحقول في سجل الأمان من اليسار إلى اليمين عبر الصفحة. إن نص سجل الأمان هو قائمة حيوية، حيث يتم إدخال البيانات عند أسفل السجل. يجب تحديد أحد خياري التسجيل أو كليهما ليتم إدخال البيانات ضمن سجل الأمان.

لتمكين خيارات تسجيل الأمان:

- ا فتح اتصالات شبكة الاتصال. - انقر فوق اتصال شبكة الاتصال الذي تم تمكين جدار حماية اتصال إنترنت (ICF) عليه، ثم تحت مهام شبكة - الاتصال، انقر فوق تغيير إعدادات هذا الاتصال. - في التبويب خيارات متقدمة، انقر فوق إعدادات. - في التبويب تسجيل الأمان، تحت خيارات التسجيل، حدد واحد من الخيارات التالية أو كليهما: - لتمكين تسجيل محاولات الاتصال الوارد غير الناجحة، حدد خانة الاختيار تسجيل الحزم المسلّمة. - لتمكين تسجيل الاتصالات الصادرة الناجحة، حدد خانة الاختيار تسجيل الاتصالات الناجحة.

تكوين الشبكة المنزلية او المكتبية وتزويدها بالجدار الناري الداعم:

لم تكن شبكة الاتصال المنزلية أسهل مما هي عليه الآن في Windows XP Professional. يمكن استخدام معالج إعداد شبكة الاتصال لإعداد الشبكة الخاصة بك بسرعة. يمكن مشاركة الاتصال بالإنترنت مع كافة أجهزة الكمبيوتر على الشبكة الخاصة بك وكن مرتاحاً لحماية الكمبيوتر الخاص بك من قبل جدار حماية اتصال إنترنت.

إعداد شبكة الاتصال المنزلية أو المكتبية الصغيرة :

يرشدك معالج إعداد شبكة الاتصال خلال تكوين شبكة الاتصال المنزلية أو المكتبية الصغيرة. يمكن إعداد كافة أجهزة الكمبيوتر على الشبكة الخاصة بك لتستخدم اتصالاً وحيداً بالإنترنت، وتسمية كل كمبيوتر أو تزويده بوصف، وتمكين جدار حماية اتصال إنترنت. يمكنك استخدام معالج إعداد شبكة الاتصال فقط بعد إعداد أجهزة الكمبيوتر وتوصيلها فعلياً.

الإنشاء السهل لشبكة الاتصال المنزلية :

هل تريد مزيداً من المعلومات حول جدوى إعداد شبكة اتصال، وكيفية ذلك؟ في حال وجود جهازي كمبيوتر أو أكثر في المنزل أو في المكتب الصغير، فإن وصلها كشبكة اتصال يزيد من إمكانياتها وربما يوفر عليك المال. عند إعداد شبكة اتصال، يمكن مشاركة الأجهزة (مثل الطابعات والماسحات الضوئية)، ومشاركة اتصال وحيد بالإنترنت، ومشاركة الملفات والمجلدات. يمكن أيضاً تشغيل التسالي التي تعمل على أجهزة كمبيوتر متعددة. يرشدك Windows XP Professional خطوة بخطوة خلال عملية إعداد شبكة الاتصال المنزلية أو المكتبية الصغيرة. شبكة الاتصال هي أكثر من مجرد مجموع مكوناتها. يمكن لأجهزة الكمبيوتر على شبكة اتصال مشاركة اتصال إنترنت، والطابعات وأجهزة أخرى، وعرض الملفات بشكل مشترك. ويمكنك استخدام شبكة الاتصال كذلك للعب ألعاب الكمبيوتر

متعددة اللاعبين. إن ربط أجهزة الكمبيوتر لتشكيل شبكة اتصال يزيد كثيراً من إمكانياتها ويمكن أن يوفّر نقودك! هل يحتوي بيتك على جهازي كمبيوتر أو أكثر؟ عن طريق وصلها بشبكة اتصال، يمكنك:

- أن تتشارك باتصال إنترنت وحيد. يملك Microsoft® Windows® XP ميزة تدعى مشاركة اتصال إنترنت (ICS). وباستخدام ICS، يشارك كمبيوتر واحد، يدعى مضيف ICS، اتصال إنترنت الخاص به مع باقي أجهزة الكمبيوتر على شبكة الاتصال. وعن طريق مشاركة اتصال إنترنت وحيد، يمكنك بشكل متزامن التنقل في ويب على جهازك بينما يقوم فرد آخر من العائلة بمراجعة البريد الإلكتروني على كمبيوتر آخر.

- أن تتشارك بالطابعة، والماسح، والأجهزة الأخرى. قد يكون لديك طابعة متصلة بكمبيوتر في غرفة أخرى. باستخدام شبكة الاتصال المنزلية، يمكنك الطباعة على هذه الطابعة من الكمبيوتر الذي في غرفتك. لم تعد بحاجة إلى نسخ الملف على قرص مرن وأخذه إلى الكمبيوتر الذي يملك الطابعة.

- أن تتشارك بالملفات والمجلدات. افرض أن ابنك طلب إليك النظر إلى تقرير مدرسي موجود على الكمبيوتر في غرفة نومه. عندما تكون أجهزة الكمبيوتر مرتبطة بشبكة اتصال يمكنك، على سبيل المثال، فتح الملف من جهازك، وإجراء التغييرات، ثم حفظ الملف على كمبيوتر ابنك.

- أن تلعب ألعاب الكمبيوتر متعددة اللاعبين. عن طريق شبكات الاتصال ومشاركة اتصال إنترنت، يمكن لأفراد العائلة أن يلعبو ألعاباً على أجهزة كمبيوتر منفصلة مع بعضهم أو على إنترنت. وبينما هم يلعبون، يمكنك أيضاً التنقل في ويب — على سبيل المثال، زيارة مواقع الرياضة والمال المفضلة لديك.

وهناك المزيد: يجعل Microsoft Windows XP استخدام شبكات الاتصال أسهل من أي وقت مضى. ولكن عليك أولاً ربط أجهزة الكمبيوتر ببعضها، عن طريق تثبيت الأجهزة المناسبة في كل منها وعن طريق وصلها بالأسلاك أو بوسائط التقنية اللاسلكية. تشرح هذه المقالة العملية من البداية إلى النهاية. ستتعلم كيف تختار تقنية شبكة الاتصال المناسبة لبيتك، والمكوّنات المناسبة التي يجب الحصول عليها، وكيفية تثبيتها ووصلها بالشكل المناسب. وهناك أيضاً قسم حول حماية شبكة الاتصال المنزلية من المتطفلين الخارجيين عن طريق إنشاء حاجز آمن يدعى جدار الحماية، وهو نفسه الذي يُستخدم في مجال الأعمال.

مشاركة اتصال إنترنت :

استخدم مشاركة اتصال إنترنت لوصل أجهزة كمبيوتر شبكة الاتصال المنزلية بإنترنت بواسطة اتصال وحيد فقط. بواسطة مشاركة اتصال إنترنت، يمكن استخدام برامج استعراض إنترنت وخدمات البريد الإلكتروني من أي كمبيوتر على شبكة الاتصال الخاصة بك، حتى وإن لم يكن ذلك الكمبيوتر موصولاً بالإنترنتز يمكنك بواسطة مشاركة الاتصال بإنترنت (ICS) الاتصال بأجهزة الكمبيوتر الموجودة على الشبكة المنزلية أو المكتبية الصغيرة بإنترنت باستخدام اتصال واحد فقط. على سبيل المثال، لديك كمبيوتر واحد متصل بإنترنت باستخدام اتصال الطلب الهاتفي. وعند تمكين ICS على هذا الكمبيوتر، حيث يدعى مضيف ICS، ستتصل أجهزة الكمبيوتر على شبكة الاتصال بإنترنت باستخدام اتصال الطلب الهاتفي هذا. عند إعداد الشبكة المنزلية أو المكتبية الصغيرة، فمن المستحسن استخدام معالج إعداد شبكة الاتصال في Windows XP Professional لتمكين مشاركة الاتصال بإنترنت. يوفر معالج إعداد شبكة الاتصال تلقائياً كافة إعدادات شبكة الاتصال التي تحتاجها لمشاركة اتصال واحد بإنترنت مع كافة أجهزة الكمبيوتر الموجودة على شبكة الاتصال. بعد تمكين ICS، وبعد التأكد من أن كافة أجهزة الكمبيوتر لديك يمكنها الاتصال مع بعضها ومن أنه يمكنها الوصول إلى إنترنت، يمكنك استخدام برامج مثل Internet Explorer و Outlook Express كما لو أنه تم وصلها مباشرةً مع موفر خدمة إنترنت (ISP). عند إجراء طلب لإنترنت، يتصل كمبيوتر المضيف ICS بـ ISP ويقوم بإنشاء اتصال بحيث تتمكن أجهزة الكمبيوتر الأخرى من الوصول إلى عنوان معين على ويب أو من تحميل بريد إلكتروني. لاختبار اتصال إنترنت والشبكة لديك، تأكد من أنه يمكنك مشاركة الملفات بين أجهزة الكمبيوتر ومن إمكانية كل كمبيوتر من الوصول إلى عنوان ويب. إن مشاركة الاتصال بإنترنت مخصصة للاستخدام في شبكة الاتصال حيث يوجه الكمبيوتر المضيف ICS اتصالات الشبكة بين أجهزة الكمبيوتر وإنترنت. من المفترض أنه في الشبكة المنزلية أو المكتبية الصغيرة، أن يكون لدى الكمبيوتر

المضيف ICS اتصال إنترنت الوحيد. بينما قد يكون لدى أجهزة الكمبيوتر الأخرى أجهزة مودم للوصول إلى إنترنت، ويكون الاتصال الأساسي الخاص بهم عبر الكمبيوتر المضيف ICS. عليك تمكين ICS على الاتصال العمومي للشبكة المنزلية أو المكتبية الصغيرة. إذا كان لديك أكثر من محول شبكة اتصال واحد مثبت على الكمبيوتر، فعليك اختيار اتصال الشبكة المحلية الذي يتصل بباقي أجهزة الكمبيوتر على الشبكة المنزلية أو المكتبية الصغيرة. ويدعى هذا أيضاً باتصال شبكة الاتصال الخاصة. إذا تواجد اتصالي شبكة محلية أو أكثر، فعند تمكين ICS، عليك القيام بواحد مما يلي:

حدد اتصال واحد للاتصال بباقي أجهزة الكمبيوتر الموجودة على شبكة الاتصال. لمزيد من المعلومات حول كيفية اختيار الاتصال الخاص، راجع اتصالات شبكة الاتصال الخاصة والعامة. إذا كان لديك اتصالين محليين أو أكثر، وكان جميعها يتصل بباقي أجهزة الكمبيوتر الموجودة على شبكة الاتصال لديك، فعليك استخدام جسر لوصل الاتصالات المحلية قبل تحديد الاتصال بالشبكة المنزلية أو المكتبية الصغيرة. إذا اخترت إنشاء جسر شبكة اتصال يتضمن كافة الاتصالات المحلية بشبكة الاتصال لديك، فيتم تحديد الجسر تلقائياً عند تمكين ICS. وإذا قمت بإنشاء جسر شبكة اتصال لا يتضمن كافة الاتصالات المحلية بشبكة الاتصال لديك، يبقى بإمكانك تحديد الجسر كاتصال خاص.

جدار حماية اتصال إنترنت

يعمل جدار حماية اتصال إنترنت كنظام أمان، يحدد المعلومات المتبادلة من أجهزة الكمبيوتر على شبكة الاتصال الخاصة بك إلى إنترنت، ومن إنترنت إلى أجهزة الكمبيوتر على شبكة الاتصال لديك، يمكن أيضاً تمكين جدار حماية اتصال إنترنت على كافة أجهزة الكمبيوتر على شبكة الاتصال الخاصة بك، حتى وإن كانت أجهزة الكمبيوتر تشترك باتصال وحيد بالإنترنت.

تمت بحمد الله .

أعداد المبرمج :مشتاق طالب رشيد العامري

Mushtaq_talib58@yahoo.com